Claims:

1. A method comprising the steps of:

monitoring access points through which data can be exchanged with a network,

identifying an unauthorized access point, and

monitoring traffic passing through the identified unauthorized access point.

2. A method according to Claim 1 further comprising the step of determining the geographical location of the identified unauthorized access point.

3. A method according to one of Claims 1 and 2 further comprising the step of applying traffic filtering to monitored traffic passing through the identified unauthorized access point.

4. A method according to one of Claims 1, 2 and 3 further comprising the steps of:

responding to the identification of an unauthorized access point by determining the make, model and default configuration password for the unauthorized access point, and

addressing the unauthorized access point using the default password and, on gaining access thereto, reconfiguring the access point into an authorized access point.

5. A method according to one of Claims 1 through 4 further comprising the step of accumulating charges for access and usage of network resources identified to the identified unauthorized access point.

6. A method according to one of Claims 1 through 5 wherein the step of identifying an unauthorized access point comprises comparing the identity of

monitored access points with a database of authorized access points.

7. A method according to Claim 6 wherein the step of monitoring comprises equipping each of a plurality of computer devices to detect access points accessible to the device and to report to a server computer system the identity of detected access points.

8. A method according to Claim 6 wherein the step of monitoring comprises querying network nodes for recent entries into node identifying connectivity tables maintained at the nodes.

9. A method according to one of Claims 7 and 8 wherein the step of monitoring is performed intermittently and periodically.

10. A method according to Claim 9 wherein the step of monitoring is performed at predetermined regular intervals.

11. A method according to Claim 9 wherein the step of monitoring is performed at random irregular intervals.

12. A method according to Claim 2 wherein the step of determining the geographic location of an identified unauthorized access point comprises comparing the locations of a plurality of computer devices all of which report detection of the identified unauthorized access point.

13. A method according to Claim 3 wherein the step of applying traffic filtering comprises denying access to the network through the identified unauthorized access point.

14. Apparatus comprising:

a computer system;

a network interface connected to said system and providing a communication channel between said system and a network; and

program instructions stored accessibly to said computer system and cooperating with said computer system when executing on said computer system to monitor access points through which data can be exchanged with a network, assist in identifying an unauthorized access point, and monitor traffic passing through an identified unauthorized access point.

15. Apparatus according to Claim 14 wherein said computer system is a workstation computer system and further wherein said program instructions include an access point identification program cooperating therewith when executing on said system to identify access points accessible through said interface; and a reporting program cooperating with said identification program and with said system when executing on said system to report through said interface to a remote server computer system the identity of accessed points.

16. Apparatus according to Claim 14 wherein said computer system is a server computer system and further wherein said program instruction include a node identification database cooperating therewith when said program is executing on said system to identify unauthorized access points accessible to said system through said interface.

17. Apparatus according to one of Claims 15 and 16 and further comprising a geographical location determining program effective when executing to derive the physical location of an unauthorized access point.

18. Apparatus according to one of Claims 15 through 17 and further comprising a traffic filter controlling program effective when executing to selectively impose a filter on traffic exchanged with the network through an unauthorized node.

19. Apparatus according to one of Claims 15 through 18 and further comprising a control program effective when executing to respond to the identification of an unauthorized access point by determining the make, model and default configuration password for the unauthorized access point, address the unauthorized access point using the default password and, on gaining access thereto, reconfigure the access point into an authorized access point.

20. Apparatus according to one of Claims 15 through 19 and further comprising an accounting control program effective when executing to accumulate charges for access and usage of network resources identified to the identified unauthorized access point.

21. A program product comprising:

a computer readable medium; and

program instructions stored on said medium accessibly to a computer system and effective when executing on a system to:

monitor access points through which data can be exchanged with a network,

identify an unauthorized access point, and

monitor traffic passing through the identified unauthorized access point.

22. A program product according to Claim 21 wherein the program instructions further comprise instructions effective to determine the geographical location of the identified unauthorized access point.

23. A program product according to one of Claims 21 and 22 wherein the program instructions further comprise instructions effective to apply traffic filtering to monitored traffic passing through the identified unauthorized access point.

24. A program product according to one of Claims 21, 22 and 23 wherein the

program instructions further comprise instructions effective to respond to the identification of an unauthorized access point by determining the make, model and default configuration password for the unauthorized access point, and address the unauthorized access point using the default password and, on gaining access thereto, reconfigure the access point into an authorized access point.

25. A program product according to one of Claims 21 through 24 wherein the program instructions further comprise instructions effective to accumulate charges for access and usage of network resources identified to the identified unauthorized access point.

26. A program product according to one of Claims 21 through 25 wherein the program instructions further comprise instructions effective to compare the identity of monitored access points with a database of authorized access points.